**Amendments to the Claims:**

This listing of claims will replace all prior version, and listings, of claims in this application:

**Listing of Claims**

Claims 1-17: cancelled.

Claim 18. (Previously Presented) A method for securing a token from unauthorized use, comprising:

intercepting by a hub a first message from the host processing device addressed to the token in ~~a~~ the hub;

providing by the hub the intercepted message to a PIN entry device communicatively coupled to the hub, the PIN entry device being different from a keyboard associated with the host processing device;

accepting by the hub a second message from the PIN entry device comprising a user-entered PIN;

generating by the hub a third message from the second message, the third message comprising the user-entered PIN and at least a portion of the first message; and

transmitting the third message from the USB-compliant hub to the token.

Claim 19. (Original) The method of claim 18, further comprising the step of:

encrypting the third message according to a first encryption key stored in a memory of the token before transmitting the third message to the token.

Claim 20. (Previously Presented) An apparatus for securing a token from unauthorized use, comprising:

a USB-compliant hub, communicatively coupleable between a host processing device and the token, the USB-compliant hub having:

means for intercepting a message addressed to the PIN entry device;

means for generating a third message from the first message and a user-entered PIN; and

means for transmitting the third message to the token; and

a PIN entry device, communicatively coupled to a USB-compliant hub, for accepting a user-entered PIN and providing the user-entered PIN to the USB-compliant hub, the PIN entry device being different from a keyboard associated with the host processing device.

Claim 21. (Original) The apparatus of claim 20, wherein the means for intercepting a message addressed to the PIN entry device, the means for generating the third message from the first message and a user-entered PIN and the means for transmitting the third message to the token comprises at least one processor having at least one communicatively coupled memory storing processor instructions for intercepting a message addressed to the PIN entry device, for generating the third message from the first message and a user-entered PIN, and for transmitting the third message to the token.

Claim 22. (Original) The apparatus of claim 20, wherein the USB-compliant hub further comprises a means for encrypting the third message according to an encryption key stored in a memory of the token.

Claim 23. (Original) The apparatus of claim 22, wherein the means for intercepting a message addressed to the PIN entry device, the means for generating the third message from the first message and a user-entered PIN, the means for encrypting the third message according to an encryption key stored in the memory of the token and the means for transmitting the third message to the token comprises at least one processor having at least one communicatively coupled memory storing processor instructions for intercepting a message addressed to the PIN entry device, for generating the third message from the first message and a user-entered PIN, for encrypting the third message according to an encryption key stored in the memory of the token and for transmitting the third message to the token.